Before the

Federal Communications Commission

Washington, D.C. 20554

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate	)	CG Docket No. 17-59
Unlawful Robocalls	)	

Comments of AARP

July 24, 2019

Trevor R. Roycroft, Ph.D.
Economic Consultant

David Certner
Legislative Counsel and
Legislative Policy Director
Government Affairs
AARP
601 E Street, NW
Washington, DC 20049

Table of Contents

Introduction and summary of recommendations 1
Consumers must be informed of continuing robocall risks 4
Consumers should have clear notice regarding network blocking 5
Uniform display information will reduce customer confusion 6
Callers who have been erroneously blocked should be able to easily recover 7
Blocking programs should be free of charge to consumers 9
To ensure the rapid deployment of reliable blocking technology, all service providers should be compliant 10
Initial safe harbors should be conservative 10
White lists should not be utilized until authentication is ubiquitous and then with caution 11
Calls placed to 911 must go through in all cases 12
Legitimate use of autodialing technology should be protected 12
Service provider robocall blocking systems should be hardened against cyberattacks 13
Conclusion 13

Introduction and summary of recommendations

AARP respectfully submits these Comments for the FCC's consideration, and thanks the Commission for the opportunity to participate in this important proceeding regarding the blocking of robocalls. The *Declaratory Ruling and Third Further Notice of Proposed Rulemaking* (hereinafter *FNPRM*) marks another milestone in the FCC's efforts to crack down on unwanted calls and the scourge of illegal robocalls.[1] The Commission has previously recognized that call blocking is serious business: "call blocking poses a threat to the ubiquity and seamlessness of the network, the Commission has long had a strong policy against allowing voice service providers to block calls."[2] While the *FNPRM* states that it expects "the vast majority" of blocked calls to be illegitimate,[3] the *FNPRM* also indicates that it is unlikely that the system will be error free.[4] This fact supports the proposition that consumer protection is imperative in light of the new "blocking" public switched telecommunications network (PSTN).

At some point in the future AARP hopes that all illegal robocalls are eliminated. However, as noted in the *FNPRM*, the current patchwork quilt of blocking-compatible IP-based voice networks and blocking-incompatible TDM-based voice networks does not currently enable the blocking of all robocalls.[5] For blocking to be successful, the *FNPRM* indicates that each intermediate provider on a call path must accurately pass authenticating information to the

[1] Because the scope of the *FNPRM* now extends beyond robocalls that are illegal, AARP will conserve notation in these comments by referring to unwanted calls and illegal robocalls simply as "robocalls." AARP considers "unwanted calls" to be automatically dialed calls that are made to a consumer who *has not provided prior consent*.
[2] *In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls*, CG Docket No. 17-59, Notice of Proposed Rulemaking and Notice of Inquiry, March 23, 2017, ¶4.
[3] *FNPRM,* ¶51.
[4] *FNPRM,* ¶52.
[5] *FNPRM,* ¶21, footnote 43: "We note that SHAKEN/STIR as developed is intended for IP networks. As a result, calls that originate, transit, or terminate on TDM networks may not benefit from it." ¶80 "As explained earlier, SHAKEN/STIR as developed is intended for IP-based networks, and thus, is less effective for calls that originate, terminate, or transit across TDM networks and does not work at all for calls that exclusively traverse TDM networks."

terminating provider, and also notes that not all providers will be able to perform that task for some time.[6] Furthermore, even if the domestic robocall blocking system were to be perfected, internationally sourced robocalls will continue to be difficult to block.[7] It is also reasonable to expect that the game of cat and mouse between robocallers and service providers who attempt to block robocalls will continue for an extended period as robocallers will seek and exploit weaknesses in robocall blocking systems. Blocking failures may expose consumers to both continuing receipt of robocalls and also the potential for their own calls to be blocked as false positives.

As a result of these significant changes, consumer protection and education are imperative. New choices, such as opt-out blocking services[8] and opt-in white lists[9] should be fully explained to consumers, including the potential consequences of adopting, or not adopting, the new technologies. Also, blocking solutions are likely to be less-than perfect for an extended period, including the possibility for false positives that may result in legitimate callers being blocked, which could easily lead to service disruptions and customer confusion. All of these factors point to the importance of accurate information and educational materials being provided to consumers. In light of the significant changes to the PSTN that are emerging as a result of the Commission's robocall blocking efforts, AARP recommends the following:

- The Commission should establish customer notice rules that will result in clear statements from service providers to their customers regarding the abilities and

[6] *FNPRM,* ¶67 "We recognize that all or part of some voice service provider networks are not IP-based. In these instances, deployment of authentication technology may be delayed."
[7] "iconectiv notes that implementation of SHAKEN/STIR in the U.S. will allow traceback of all calls to the point of entry onto the U.S. network for international calls. However, they point out that there could still be significant difficulty tracing international calls back to their point of origin absent international implementation of the standards." *FNPRM,* ¶50, footnote 103.
[8] *FNPRM,* ¶31.
[9] *FNPRM,* ¶46.

weaknesses of their blocking technologies. AARP urges the Commission to introduce consumer representation into the oversight of its robocall blocking programs.

- The Commission should require service providers to establish robust and comprehensive customer outreach and support efforts associated with their robocall blocking technology. Service providers should be required to adequately train their customer service representatives so that accurate information is provided to consumers. Customer notification regarding robocall blocking should be standardized to ensure that consumers can easily recognize differences in blocking technologies utilized by various service providers.

- The Commission should work to standardize information conveyed to consumers from the network regarding the status of incoming calls. Degrees of call attestation should be clearly and consistently displayed across service providers so consumers can make appropriate choices when deciding whether to answer a call.

- Callers should receive easy-to-understand feedback from the network when their call is blocked as a robocall and should be able to easily remedy inadvertent or inappropriate blocking. Customer notification should include standardized error codes or other network feedback that will allow a blocked caller to convey what they are experiencing to customer service representatives.

- There should be no charge to customers for call blocking technology. Free and ubiquitously available blocking technology will ensure that there are no targets for robocallers and will more effectively undermine the business model of robocallers.

- The Commission should move as quickly as possible to require all service providers to deploy robocall blocking technology. Because the potential for success of robocall blocking technology is related to the weakest link in the network of networks that makes up the PSTN, the faster the FCC gets all service providers into compliance with technology deployment milestones, the more quickly effective blocking of robocalls can begin.

- Because of uncertainty regarding how robocall blocking technology will initially perform, AARP believes that the Commission should establish a safe harbor "glide path" that should initially discourage overly aggressive blocking. As the industry identifies and corrects implementation and operational problems with robocall blocking technology, the Commission can then move to strengthen the safe harbor provisions.

- AARP is concerned that universal white lists could be compromised and undermine the effectiveness of both emergency call distribution systems and robocall blocking. AARP believes that universal white lists should not be implemented until caller ID authentication has been fully implemented, including calls originating overseas.

- No calls to 911 should ever be blocked.

- AARP encourages the Commission to establish mechanisms that provide prompt recourse for legal callers who use auto dialers and who establish prior consent with call recipients, should they be blocked as robocallers. AARP urges the Commission to define "unwanted calls" as autodialed calls that are made without prior consent.

- AARP agrees with the *FNPRM* that analytics-based robocall blocking must be applied in a non-discriminatory and competitively neutral manner.

- Because robocall blocking technology has the potential to disrupt the operations of the PSTN, AARP urges the Commission to ensure that best practices are followed by service providers to protect robocall blocking systems from cyberattacks.

In the sections that follow AARP expands on these recommendations.

Consumers must be informed of continuing robocall risks

The introduction of new technologies, such as SHAKEN/STIR, and new approaches to implementation, such as the *Declaratory Ruling's* decision to allow service providers to make robocall blocking programs the default, can easily be misunderstood by consumers as indicators that they no longer need to be cautious regarding the calls that they receive. That false sense of security could easily lead to increased willingness of consumers to respond to callers that may ultimately be fraudulent due to the inability of service providers to block all illegal robocalls. Consumers must be informed of the ongoing risks of robocalls that will linger for the foreseeable future. The Commission should also require service providers to not overstate the capabilities of robocall blocking technology. No service provider will be able to claim that all robocalls will be blocked, at least not initially.[10] It is not reasonable for the shortfalls of a service provider's robocall blocking technology to go unstated or to appear in the "fine print" in an advertisement touting the virtues of that service provider's blocking technology. The Commission should work

[10] See, *supra* notes 5, 6, and 7.

with consumer groups and service providers to develop standardized notification and information-distribution methods. Customer notification regarding robocall blocking should be standardized to ensure that consumers can easily recognize differences in blocking technology utilized by various service providers.

Consumers should have clear notice regarding network blocking

The network changes required in the *Declaratory Ruling* are significant and customer notice regarding the changes is important so that consumers understand what their service is doing to the calls that they send and receive, and what they must do to either activate or avoid robocall blocking technologies, depending on their preferences. The new "blocking" PSTN is more complex than the previous PSTN generation. For example, the fact that SHAKEN/STIR provides "three levels of attestation: full, partial, and gateway"[11] is information that is critical for consumers to understand the degree of protection associated with robocall blocking technology. The differences between these levels of attestation are likely to be difficult for consumers to appreciate unless service providers provide consumers with easy-to-understand information about the degree of protection associated with an incoming call. The *Declaratory Ruling* indicates that notification about network changes can come through postings on a service provider's web site, through text message or email, or bill insert.[12] These delivery mechanisms are not enough. The Commission should require service providers to establish robust and comprehensive customer outreach and support efforts.

[11] *FNPRM,* ¶67.
[12] *FNPRM,* ¶33.

As the *FNPRM* notes, robocall blocking technology is complex;[13] consumer education will be essential during the transition period. For example, in addition to the methods described in the *FNPRM,* service providers should provide educational outreach to national, regional, community, and governmental entities whose members or constituencies need to be educated about how robocall blocking technology works, and how to quickly resolve problems that may be associated with false positives. Service providers should also provide online tutorials for consumers regarding blocking technologies and advanced training for customer service representatives that will ensure that those customer service representatives provide consistent and accurate information on robocall blocking technology.

Uniform display information will reduce customer confusion

The *FNPRM* asks whether the Commission should require providers to adopt a uniform display to provide consumers information on whether a call has been authenticated.[14] AARP believes that a uniform display for call authentication is a good idea. Consumers may rely upon multiple voice service providers and receiving standardized call display information would improve the effectiveness of robocall blocking technology and empower consumers to make choices regarding calls that they are receiving. Relying on preexisting terminology or symbols to categorize information about the degree of certainty that a call is not a robocall may be useful. For example, the level of call attestation could be conveyed to consumers through a "Green Light," "Yellow Light," "Red Light" framework, with full attestation delivering a "Green Light" symbol to consumers. Partial or Gateway attestation could be associated with the "caution"

[13] *FNPRM,* ¶67.
[14] *FNPRM,* ¶77.

symbol of a "Yellow Light" and unattested calls would receive a "Red Light."[15] Alternatively, a new system of symbols, in the spirit of universal hazard symbols, could be created to convey the degree of risk associated with an incoming call. The Commission should establish and facilitate a working group that includes representatives of consumer groups to establish basic design elements of display information.

Callers who have been erroneously blocked should be able to easily recover

AARP is concerned that while the Commission has now taken steps to make the widespread deployment of robocall blocking technology a reality, the Commission has yet to establish a mechanism that would allow legitimate callers who have been blocked due to blocking errors,[16] service provider non-compliance,[17] service provider mistakes,[18] or other potential causes of false positives, to quickly recover their services. Given potentially inconsistent practices of various service providers it is conceivable that, either due to technological incompatibility or errors on the part of an originating service provider, a consumer may be unable to complete calls that terminate on the network of another service provider. For example, the *FNPRM* notes that call authentication may fail due to a voice service provider failing to update its signing certificate.[19] Similarly, calls that originate on or transit TDM-based networks may have authentication difficulties.[20] The vagaries of the routing of calling traffic may generate calling outcomes that

[15] These symbols could be accompanied by text that stated "Stop/Caution/Go" as appropriate to provide additional information to those who have difficulty seeing colors. Consumers should have the ability to see calling numbers and the degree of attestation as an option, in addition to the outright blocking of all calls lacking attestation.
[16] *FNPRM*, ¶33, footnote 72.
[17] *FNPRM,* ¶54. "If other large voice service providers with the technical capacity to implement the SHAKEN/STIR framework on a similar timeline fail to do so, should blocking unsigned calls from such voice service providers, after a reasonable transition period, fall within the safe harbor?"
[18] *FNPRM*, ¶52.
[19] *FNPRM,* ¶52.
[20] *FNPRM,* ¶80.

are difficult for service providers to troubleshoot and virtually impossible for consumers to understand. A call that successfully completes one day may be blocked the next day due to differences in the way that the call is routed or due to the expiration of a signing certificate.[21]

Callers should receive easy-to-understand feedback from the network when their call is blocked as a robocall.[22] While the Commission has encouraged service providers to "develop a mechanism for notifying callers that their calls have been blocked,"[23] absent rules on this matter consumers may face a confusing web of contradictory notifications (or lack of notification) and finger-pointing on the part of service providers. The Commission should require that the industry develop standardized methods for customer notification that their calls have been blocked. Customer notification should include standardized error codes or other network feedback that will allow the blocked caller to convey what they are experiencing to customer service representatives. Access to customer service representatives should be available to consumers even if their number has been blocked. In addition, web- and app-based methods to report blocking should be available, with online mechanisms established for consumers to authenticate their identity and verify that they "are not a robot" placing robocalls.

The *FNPRM* notes that the "industry has been active in developing solutions that allow callers to communicate with voice service providers and analytics companies to identify themselves and share their call patterns that might otherwise seem to indicate illegal call activity."[24] AARP is heartened to hear that this activity is ongoing, but absent requirements from this Commission for

[21] As noted in the *FNPRM,* ¶80, SHAKEN/STIR "is less effective for calls that originate, terminate, or transit across TDM networks."
[22] *FNPRM,* ¶52.
[23] *FNPRM,* ¶38.
[24] *FNPRM*, ¶80.

standardized and ubiquitous methods for consumers to recover from false positives it is likely that consumers will be harmed as the new systems of robocall blocking come online.

Blocking programs should be free of charge to consumers

AARP agrees with Commissioners Rosenworcel and Starks when they insist that the solution to robocalls should be free of charge.[25] Service providers should be prohibited from charging for robocall blocking technology. Failure to require all service providers to deliver robocall blocking technologies needed by consumers free of charge would be unfair to consumers, who would be placed in the undesirable position of needing to pay extra to avoid network defects. Furthermore, blocking fees would create perverse incentives for service providers to create a "baseline" network experience that was rife with robocalls, so as to make a costly blocking option more attractive to consumers. In addition, given the lack of certainty regarding the effectiveness of the blocking technology, especially during the transition period prior to all domestic service providers implementing SHAKEN/STIR, charging for a service that is unlikely to block all robocalls would be unfair to consumers. Finally, free and ubiquitously available blocking technology will more effectively undermine the business model of robocallers. To the extent that a portion of network users are not protected due to blocking technology that is costly to consumers, robocallers will continue to have targets. Robocall blocking technology that is freely available to all network users will better reduce the number of unprotected consumers who would be easy prey for robocallers.

[25] *FNPRM,* Statement of Commissioner Jessica Rosenworcel. Statement of Commissioner Geoffrey Starks.

To ensure the rapid deployment of reliable blocking technology, all service providers should be compliant

The *FNPRM* proposes an end-of-year 2019 deadline for major service providers to comply with SHAKEN/STIR,[26] which is appropriate, as is the *FNPRM's* proposal to initially utilize the 14 providers identified by Chairman Pai.[27] However, the Commission should ensure that the 2019 deadline is satisfied with compatible and interoperable deployments by the service providers so that by the end of 2019 there will be a seamless SHAKEN/STIR call blocking system for all major service providers. Additionally, the Commission should also address "non-major voice service providers." Because the potential for the blocking of robocalls is related to the weakest link in the network of networks that makes up the PSTN, the faster the FCC gets all service providers into compliance with technology deployment milestones, the more quickly effective blocking of robocalls can begin. Uniform blocking technology deployment will also minimize customer confusion and the potential for harm to consumers who may have their calls inappropriately blocked.

Initial safe harbors should be conservative

AARP encourages the Commission to move conservatively with regard to the establishment of safe harbors. As discussed above, the full implementation of global IP-based call authentication technology is likely to take years. In the intervening period, it is all but certain that unanticipated glitches with implementation could result in significant numbers of legitimate calls being blocked under some of the *FNPRM's* proposed safe harbor options. Given the uncertainty regarding system performance, it would be reasonable for the Commission to establish a safe

[26] *FNPRM,* ¶72.
[27] *FNPRM,* ¶73, i.e., AT&T Services, Inc., Bandwidth Inc., CenturyLink, Charter Communications, Comcast Corporation, Cox Communications, Frontier Communications, Google LLC, Sprint, TDS Telecommunications LLC, T-Mobile USA, Inc., U.S. Cellular Corp, Verizon, and Vonage Holdings Corp.

harbor "glide path" that moved to progressively more comprehensive blocking requirements as the technology improves and glitches are worked out. For example, begin by targeting the "low hanging fruit" with a safe harbor of blocking "those voice service providers that do not appropriately sign calls and do not participate in the Industry Traceback Group."[28] Over time, as the industry identifies and corrects implementation and operational problems with robocall blocking technology, the Commission can move to strengthen the safe harbor provisions, with an ultimate objective of a safe harbor that blocks calls that fail the Caller ID authentication framework under SHAKEN/STIR, or its successor.

White lists should not be utilized until authentication is ubiquitous and then with caution

The FNPRM acknowledges that certain callers should never be blocked, such as public safety answering points (PSAPs, also known as 911 call centers) and considers the creation of a "white list" that would be maintained by service providers so that they would never block one of the protected numbers.[29] AARP is concerned about this element of the robocall problem. While it is essential that emergency calls are not blocked, the creation of a universal white list introduces a significant security problem, as is indicated by the questions posed by the *FNPRM.*[30] For example, if each voice service provider maintains its own white list, the chances that at least some white lists could be compromised by robocallers would appear to increase, as the numerous contact points with white list control could be vulnerable to security breaches arising from either within or external to the service provider. On the other hand, a centrally maintained white list would present robocallers with a target that literally provided "the keys to the kingdom." Should

[28] *FNPRM,* ¶55.
[29] *FNPRM,* ¶63.
[30] *FNPRM,* ¶64.

emergency numbers be compromised in either case, the critical emergency functions of the PSTN will be seriously degraded. AARP believes, along with Consumers Union *et al.*, that universal white lists should not be implemented until caller ID authentication has been fully implemented, including calls originating overseas.[31]

Calls placed to 911 must go through in all cases

The *FNPRM* raises the issue of calls placed to 911. AARP believes that at this early stage of the implementation of robocall blocking technology, service providers adopting any safe harbor selected by the Commission should never block calls placed to 911. While AARP appreciates that spoofed calls to 911 -- such as those associated with "swatting" -- are an ongoing problem, service provider actions that might inappropriately block access to 911 would potentially impose very high costs on any caller who was the victim of a false positive and therefore prevented from contacting emergency services.

Legitimate use of autodialing technology should be protected

The use of autodialing technology should not be subject to a *de facto* ban due to the implementation of robocall blocking technology. To ensure the appropriate use of auto dialing technology, AARP believes that the Commission should establish enforceable rules to ensure that all non-emergency automatically dialed calls and texts continue to require the consent of the person called, and to establish rules that easily allow consumers to revoke previously granted consent. However, while the *FNPRM* uses the term "unwanted calls,"[32] it never formally defines what an "unwanted call" is. AARP believes that the Commission should define "unwanted

[31] Comments of Consumers Union; National Consumer Law Center, on behalf of its low-income clients; Consumer Federation of America; Consumer Action; National Association of Consumer Advocates; Public Citizen; Public Knowledge, *In the Matter of Advanced Methods to Target and Eliminate Unlawful Robocalls,* CG Docket No. 17-59, September 24, 2018, p. 8.

[32] See, for example, *FNPRM,* ¶¶1, 2, 5 and *passim.*

calls" as autodialed calls that are made without prior consent. Unless protections for the legitimate use of auto dialing technology are implemented, the implementation of blocking technology increases the risk that consumers will lose the opportunity to receive valuable and requested information. For example, AARP provides teletownhall services that are fully compliant with all current laws and rules to serve members who *request information* about a variety of topics, including fraud detection and prevention. The Commission should establish mechanisms that provide prompt recourse for legal callers who establish prior consent with call recipients who find they are blocked due to error or malfeasance. AARP also agrees with the *FNPRM* that analytics-based robocall blocking should be applied in a non-discriminatory and competitively neutral manner.[33]

Service provider robocall blocking systems should be hardened against cyberattacks

Finally, AARP encourages the Commission to require service providers to implement state-of-the-art security for the systems that will enable the blocking of calls. The computer systems that will enable blocking of robocalls could become the targets of hackers who could then disrupt the PSTN by gaining control of the blocking systems—either by enabling robocalls or causing calls that are not robocalls to be blocked. AARP urges that the FCC promote the security of call-blocking systems and encourage service providers to use best practices to ensure that their systems are not vulnerable to attack.

Conclusion

The Declaratory Ruling and *FNPRM* provide another milestone in the FCC's efforts to mitigate the robocall problem. The questions raised in the *FNPRM* illustrate the complexity of the issue

[33] *FNPRM*, ¶35.

and the risks to service providers, PSAPs and other government entities, and consumers in general. The FCC needs to move with care so as to protect consumers and preserve the integrity of the PSTN while implementing methods to discourage robocalls. AARP urges the Commission to adopt the recommendations contained in these comments.